(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 0 982 693 A2

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
01.03.2000 Bulletin 2000/09

(51) Int. Cl.[7]: **G07F 7/10**

(21) Application number: **99116600.0**

(22) Date of filing: **25.08.1999**

(84) Designated Contracting States:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE
Designated Extension States:
AL LT LV MK RO SI

(30) Priority: **28.08.1998 DE 19839041**

(71) Applicant:
International Business Machines Corporation
Armonk, NY 10504 (US)

(72) Inventors:
- **Hamann, Ernst-Michael**
  71034 Böblingen (DE)
- **Kaisser, Michael**
  71088 Holzgerlingen (DE)

(74) Representative:
Teufel, Fritz, Dipl.-Phys.
IBM Deutschland Informationssysteme GmbH,
Patentwesen und Urheberrecht
70548 Stuttgart (DE)

(54) Method to identify user-relevant states of the misoperation counter

(57) The present invention describes a method to identity and display states of the misoperation counter prior to input of a password. The method checks the state of the misoperation counter prior to every new password input. Each scanned state is assigned a defined state, which is signaled visually or acoustically to the user by the chipcard application prior to input of the password. The visual display is preferentially in the form of a traffic light, in which the colors green, amber and red are assigned to a defined state of the misoperation counter. The user of password-protected objects and/or applications is unambiguously informed of the state of the protective device for passwords by means of a clearly presented display. Especially after the card has been lost and then found again, the user can see whether anyone else has attempted to enter a password. Prior to the last chance of entering the correct password the user is clearly warned, and can check the input device again carefully before input.

EP 0 982 693 A2

Description

[0001] The present invention describes a system and method for unambiguous identification of the state of the misoperation counters of chipcards on input of identifying features, in particular passwords.

[0002] On secure data storage devices, such as chipcards, applications and data are protected by passwords (PIN = Personal Identification Number). The use of a password enables the authorized person to use a specific application or access protected data. The user enters the PIN in a card terminal and shortly thereafter a display indicates whether the PIN was correct. In this process the chipcard receives from the terminal, in the VERIFY PIN command, a normally 4-digit PIN, and compares the PIN with the one stored in the EPROM. If the externally transferred PIN and the stored PIN match, the state machine on the chipcard is influenced and the terminal is informed of the positive result of the comparison. The misoperation counter of the PIN is then likewise assigned its initial value (e.g. 3 or 0). If the transferred PIN does not match the PIN stored on the chipcard, the misoperation counter is decreased. When the counter has reached zero the card is blocked for any other PIN verification.

[0003] If the chipcard is lost and subsequently found again, its owner cannot check whether anyone has tried to use the card with an incorrect PIN.

[0004] The status of the chipcard is only signaled as an error message after input of the PIN. The chipcard holder is not warned prior to the last input attempt. Unintentional input errors can easily occur with case-sensitive passwords if the uppercase/lowercase shift key on the keyboard is accidentally pressed.

[0005] It is therefore the object of the present invention to deliver a system and method which avoids the above disadvantages in the state of the art.

[0006] This object is fulfilled by the characteristics of Claim 1. Further beneficial embodiments of the invention are set out in the sub-claims.

[0007] The user of password-protected objects and/or applications is unambiguously informed of the state of the protective device for passwords by means of a clearly presented display. Especially after the card has been lost and then found again, the user can see whether anyone else has attempted to enter a password. Prior to the last chance of entering the correct password the user is clearly warned, and can check the input device again carefully before input (e.g. that the shift key is set correctly or the biometric input unit is correctly connected).

On issue of the chipcard the user is forced to change the default password set up on manufacture of the card. If this prompt does not appear the first time the card is used, the user knows that someone has previously changed the password and possibly used the protected object.

[0008] The present invention indicates to the chipcard user the state of the misoperation counter before the password is entered. This is effected preferentially by way of a graphical user interface of the application. The graphical user interface may, for example, present to the user the following states in graphical form:

State 1: The card is new and is issued with a predefined password, or the password has been reset by the security officer and should be replaced by the user's own personal password.

State 2: The password was correctly entered in the course of the last scan.

State 3: The password was incorrectly entered in the course of the last scan, and at least a further two attempts to enter the correct password are possible.

State 4: The password was incorrectly entered in the course of the last scan, and only one further attempt to enter the correct password is possible.

State 5: The card is blocked and can only be reset by the user or by the security officer by means of a special reset password.

[0009] These states can be implemented by various graphical representations.

[0010] A preferred implementation is the graphical representation of a traffic light, in which the five states defined above are assigned the following graphical representations:

1. Flashing green light (state 1) - Special password mode; e.g. the card is new or the password has been reset by the security officer. The user is prompted to enter a password or to change a default password. If a password is entered incorrectly the graphical representation of state 3 or 4 is set, i.e. it is possible to make either at least two more attempts or only one more attempt to enter the correct password.

2. Green light (state 2) - The misoperation counter is at zero. The user still has the full number of preassigned attempts at entering the correct password. The misoperation counter can be set according to security requirements. The number of permitted failed attempts is usually three. This applies to EC cards and electronic wallets. Other cards, less at risk of unauthorized access, permit five or even ten attempts.

3. Amber light (state 3) - The misoperation counter has registered at least one failed attempt, but the user still has two more attempts.

4. Flashing amber light (state 4) - The misoperation counter has registered several failed attempts and only one more attempt is possible. The flashing amber light signals that the user must take greater care when entering the password. This especially applies to case-sensitive passwords.

5. Red light (state 5) - The misoperation counter is showing the maximum number of failed attempts. The card is blocked and the misoperation counter can only be reset by means of a reset password. Input of the password may be replaced by biometric input by means of fingerprint. From the fingerprint a unique key is generated, which is compared against a key stored on the chipcard. If no key - or no unique key - can be generated, the misoperation counter is increased. This also applies if an incorrect key is generated.

[0011] A further mode of graphical representation of states 1 to 5 may be display of differing background colors on the graphical user interface for password input, depending on the state of the misoperation counter. This may be based on the different colors of the traffic light scheme. The individual defined states of the misoperation counter may be graphically represented by any graphical symbols. The primary aspect to be considered in this is how easy the symbols are for the user to remember. The embodiments of the invention cited should therefore be mentioned only as preferred embodiments.

[0012] A further embodiment of the present invention involves acoustic representation of the defined states 1 to 5. In this, each state of the misoperation counter is assigned a specific tone or tone sequence (buzzing or beeping), or a short melody. No tone could be assigned to state 2. A buzz means the card is blocked. A beep signals state 3 and a warning tone signals state 4. This embodiment of the invention is particularly suitable for color-blind users. The combination of visual and acoustic representations of the states of the misoperation counter may represent a further embodiment of the invention.

[0013] All the embodiments of the present invention should have in common the prerequisite that only the authorized user can uniquely interpret the visual and/or acoustic state information relating to the misoperation counter. The chipcard manufacturer or issuer would have to issue with each chipcard a brief guide indicating which graphical and/or acoustic representation is assigned to which state of the misoperation counter. The unauthorized user can draw no benefit from the state information. A further variant may also involve graphical and acoustic state information being defined by users themselves. Each application program would then have to have functions enabling the user to select and display state information. This could be implemented by means of menu-guided user interfaces, for example.

[0014] However, all the embodiments of the invention should have in common the prerequisite that in the first state the password change function is always immediately called up, to enable the default password to be changed to a single password known only to the user. After input of the new password the misoperation counter is reset for example to state 2. As long as no password is entered the state - e.g. state 3 or 4 - is retained.

[0015] The defined states of the misoperation counter are preferentially signaled by way of a programming interface of the application.

[0016] The present invention is not only limited to chipcard systems. It can be used in any system in which access to data or applications is controlled by a misoperation counter.

Claims

1. Method to identify states of a misoperation counter, wherein the misoperation counter is installed on an intelligent data carrier and, when a defined number of failed attempts to enter an identifying feature is exceeded, bars access to the said intelligent data carrier, characterized by the following steps:

   a) Scanning of the current state of the misoperation counter.

   b) Assignment to the state scanned in step a) of a defined state in terms of the remaining available failed attempts to enter an identifying feature.

   c) Assignment of visual and/or acoustic information to the state of the misoperation counter defined in step b).

   d) Display of the visual and/or acoustic information prior to input of the identifying feature.

2. Method in accordance with Claim 1, characterized in that the intelligent data carrier is a chipcard.

3. Method in accordance with Claim 1, characterized in that the state of the misoperation counter ascertained in step a) contains information on the failed attempts already made and the remaining available attempts.

4. Method in accordance with Claim 1, characterized in that each scanned state of the misoperation counter is assigned a defined state, wherein each scanned state is assigned a newly defined state or several scanned states are assigned the same defined state.

5. Method in accordance with Claim 1, characterized

in that the defined state defines user-relevant states of the misoperation counter.

6. Method in accordance with Claim 1, characterized in that the identifying feature is a password or a biometric input.

7. Method in accordance with Claim 1, characterized in that each defined state is assigned a unique visual and/or acoustic information signal.

8. Method in accordance with Claim 1, characterized in that the scanned state of the misoperation counter may assume the following defined states:

State 1: The card is new and is issued with a pre-defined password, and is to be replaced by the user with a new password, or the password has been reset by the security officer and should be replaced by the user's own personal password.

State 2: The password was correctly entered in the course of the last scan.

State 3: The password was incorrectly entered in the course of the last scan, and at least a further two attempts to enter the correct password are possible.

State 4: The password was incorrectly entered in the course of the last scan, and only one further attempt to enter the correct password is possible.

State 5: The card is blocked and can only be reset by the user or by the security officer by means of a special reset password.

9. Method in accordance with Claim 4, characterized in that in state 1 a password change function is automatically called up and when a new password is entered state 2 is assigned.

10. Method in accordance with Claim 8, characterized in that each state 1 to 5 is assigned a unique graphical representation or acoustic signal.

11. Method in accordance with Claim 8, characterized in that each state 1 to 5 is assigned a written or textual representation.

12. Method in accordance with Claims 1 to 11, characterized in that representation of the visual information is integrated into the graphical user interface for input of the identifying feature.

13. Method in accordance with Claim 8, characterized in that the states 1 to 5 are implemented in the graphical representation of a traffic light by the color signals: flashing green, green, flashing amber, amber, and red.

14. Method in accordance with Claim 13, characterized in that state 1 is assigned a flashing green light, state 2 a green light, state 3 a flashing amber light, state 4 an amber light and state 5 a red light in the graphical traffic light display.

15. Method in accordance with Claim 8, characterized in that state 1 is assigned a flashing green light, state 2 a green light, state 3 an amber light, state 4 a flashing amber light and state 5 a red light, which is shown as the background color in the graphical user interface for input of the identifying feature.

16. Method in accordance with Claim 8, characterized in that states 1 to 5 of the respective chipcard application are signaled via the programming interface and the visual information is displayed in accordance with step d) by the chipcard application.

17. Method in accordance with Claim 1, characterized in that the user can himself or herself select defined states by way of a menu-guided user interface.

18. Chipcard for insertion in a chipcard reader, containing a storage device for storage of a data processing program containing data processing program components to implement the process steps in accordance with Claims 1 to 17, where the data processing product is executed on the chipcard.

19. Data processing program to be stored in a storage device of a data processing system containing data processing program components to implement the process steps 1 to 17, where the data processing program is executed on the data processing device.

20. Data processing program product in accordance with Claim 19, characterized in that the data processing program is a chipcard application.